1 リモートアクセスVPN環境の構築（クライアント編）

本書では, Windows XPに標準搭載されているVPNクライアント機能を使用して、Express5800/SG300とVPN環境を構築する際の設定方法について説明します。

はじめに（→２ページ）............ Express5800/SG300とWindows XPにおけるリモートアクセスVPN環境の構築について説明します。

リモートアクセスVPNの設定（→3ページ）............ リモートアクセスVPN環境の設定をするうえでの概要とその前提条件について説明します。

制限・注意事項（→4ページ）…............ VPN環境を構築する場合の制限と注意事項について説明します。

はじめに

本書では、Express5800/SG300（以降SG300と呼ぶ）とWindows XPを使用してリモートアクセスVPN環境を構築するために、Windows XP側で行う設定の手順を記載しています。

SG300は、IPSecを使用したVPN環境を構築することができます。IPSec暗号ペイロードでの暗号化アルゴリズムとしてはAES128、3DES、DESに対応しています。

本書で示しているのは、SG300とWindows XP間でリモートアクセスVPN環境を構築する手順の一例です。実環境ではネットワーク構成・セキュリティポリシー等により手順は異なります。SG300の設定方法、Management Consoleの使用方法の詳細に関してはSG300に同梱されているバックアップCD-ROM内のユーザーズガイド（¥nec¥doc¥下のPDFファイル）を参照してください。

また、SG300側でのリモートアクセスVPN環境構築の詳細に関しては、本書の姉妹編である「リモートアクセスVPNの設定（サーバ編）」を参照してください。

重要

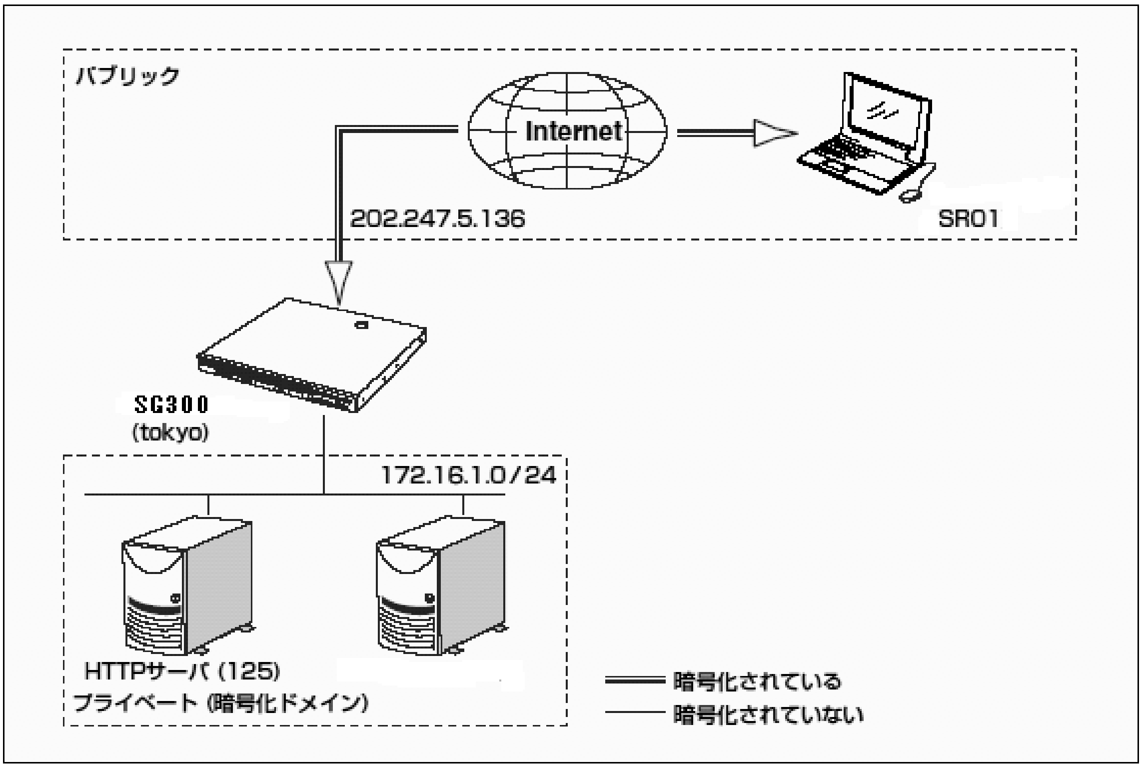
クライアント側では、Windows XPに標準搭載されている機能を利用して、リモートアクセスVPNの設定を行います。
本書では、クライアント側のOSとしてWindows XPを使用した場合を例に説明しますが、クライアント側のOSとしてWindows 2000を使用した場合でも、SG300側の設定は変わりません。同じ設定内容で接続可能です。

リモートアクセスVPNの設定

Windows XPでリモートアクセスVPN環境を設定するための概要とその前提条件を説明します。

概要

リモートアクセスVPNを構築することにより、自宅や出張先からインターネット経由で企業内ネットワークへ安全にアクセスすることが可能になります。ここでは、下図のようにWindows XPをインストールしたクライアント(SR01)とSG300内部のWebサーバ(172.16.1.0)とのデータのやり取りを暗号化するために、クライアント-SG300間でリモートアクセスVPN環境を構築するための手順を説明します。



1

VPN環境の構築について

VPN構築の前提条件

WIndows XPの設定は、OSが標準で組み込んでいるIPSec機能（セキュリティポリシー）を利用して行います。本書では、以下の条件でVPNクライアントと東京にあるローカルネットワークの間でVPN環境を構築することを前提に設定を行います。

●SG300（tokyo）側の設定

・ネットワークインタフェース

- 内側(eth0)
  IPアドレス: 172.16.1.136
  ネットマスク: 255.255.255.0
- 外側(eth1)
  IPアドレス: 202.247.5.136
  ネットマスク: 255.255.255.0

・アドレス変換（NAT/NAPT）を行う
  HTTPサーバ公開IPアドレス：202.247.5.136
  HTTPサーバ内部IPアドレス：172.16.1.125
  ネットマスク: 255.255.255.0

●Windows XP（SR01）側の設定

・クライアントネットワーク
  ネットワークアドレス：202.247.5.0
  ネットマスク: 255.255.255.0

重要

本書での設定項目は上記「VPN構築の前提条件」に則り、一例として説明しています。
個別の設定項目（IPアドレス等）は、適宜お客様の環境にあわせて設定してください。

制限・注意事項

- VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。
- VPN接続時に、停電などによりSG300の電源がOFFになると、相手側VPN機器にセキュリティアソシエーション（SA）が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。